УДК 004.056.5

А.К. Новокшонов
Київський національний університет імені Тараса Шевченка, Україна
пр. Академіка Глушкова, 4д, м. Київ, 03680

ПІДВИЩЕННЯ ІНТЕЛЕКТУАЛЬНОСТІ МОБІЛЬНИХ ПРИСТРОЇВ НА ПРИКЛАДІ АЛГОРИТМІВ ЗАХИЩЕНИХ ГРУПОВИХ КОМУНІКАЦІЙ

A.K. Novokshonov
Taras Shevchenko National University of Kyiv, Ukraine
Academician Glushkov ave., 4d, Kyiv, 03680

INCREASING INTELLIGENCE OF MOBILE DEVICES ON THE EXAMPLE OF SECURE GROUP COMMUNICATION ALGORITHMS

У роботі представлені результати аналізу ефективності алгоритмів, що підвищують інтелектуальність та захищеність мобільних пристроїв, на прикладі операцій захищених групових комунікацій з використанням структури типу бінарне дерево.
Ключові слова: мобільні пристрої, інтелектуальні алгоритми, бінарні дерева, груповий протокол Діффі-Хеллмана на основі дерева.
The paper presents results of performance analysis of the algorithms that increase intelligence and security of mobile devices by the example of secure group communications using a binary tree structure.
Keywords: mobile devices, intelligent algorithms, binary trees, tree-based group Diffie-Hellman protocol.

Вступ

Роль мобільних пристроїв, до яких відносять смартфони, планшети, «розумні» годинники тощо, у наш час важко переоцінити. Наявність миттєвого доступу до мережі Інтернет та багато корисних функцій, різноманітність мультимедіа-контенту та засобів спілкування робить такі пристрої незамінними. Технічний прогрес виробників апаратного забезпечення для мобільних платформ дозволяє покладати на мобільні пристрої все більш відповідальні функції та реалізовувати більш складні алгоритми.

Проте недоліком таких процесів є те, що рівень захищеності мобільних пристроїв не встигає за швидким технічним прогресом, що з кожним роком створює все серйозніші негативні наслідки для власників таких пристроїв. Прикладом може бути зловмисне програмне забезпечення для мобільних пристроїв, яке має на меті доступ до фінансових відомостей у мобільному банкінгу; особистих відомостей, що можуть бути використані для цілей шахрайства; обчислювальних ресурсів, що можуть використовуватися для розсилки спам-повідомлень та проведення DDoS-атак тощо.

У зв’язку з цим актуальним стає питання дослідження та реалізації ефективних алгоритмів, які змогли б як підвищити інтелектуальність мобільних пристроїв та використати всі сучасні апаратні можливості мобільних платформ, так і покращити рівень захищеності комунікацій, що здійснюються з використанням таких платформ.

Метою цієї роботи є експериментальне дослідження швидкодії алгоритмів захищених групових комунікацій, які можуть бути ефективно реалізовані для мобільних пристроїв та можуть підвищити їхню інтелектуальність з точки зору захисту комунікацій.

Алгоритми захищених групових комунікацій

Захищені групові комунікації – це сценарій, в якому сукупність довірених суб’єктів приймає участь у групових комунікаціях і потребує захисту важливих відомостей, що передаються всередині групи. Захист цих відомостей ґрунтується на володінні спільними секретними криптографічними параметрами (наприклад, знання спільного секретного ключа шифрування). При цьому зовнішні спостерігачі, які не є учасниками групи, не мають змоги розшифрувати зміст групових повідомлень, навіть якщо вони мають можливість перехоплювати зашифровані повідомлення.

Особливістю цього сценарію взаємодії є використання для комунікацій відкритих, загальнодоступних каналів зв’язку (таких, як Інтернет). Варто враховувати, що для захисту таких комунікацій від атак типу «людина посередині» (англ. man-in-the-middle attack) необхідно додатково використовувати механізми автентифікації всіх учасників групи. Додаткову інформацію щодо класифікації атак типу «людина посередині» та методів захисту від них можна знайти у [1].

Метою алгоритмів захищених групових комунікацій є створення технології для обміну криптографічними ключами між учасниками групи, які потребують утворення спільного для них секретного ключа. Далі такий ключ може бути використаний для шифрування всіх повідомлень між учасниками групи за допомогою деякого швидкого алгоритму симетричного шифрування.

Складність реалізації алгоритмів захищених групових комунікацій полягає у тому, що, по-перше, необхідно виконувати ефективне (у розумінні кількості обчислювальних операцій та кількості повідомлень, що передаються між учасниками групи) обчислення спільного групового ключа при будь-якій зміні складу групи, щоб забезпечити виконання властивостей прямої та зворотної секретності (англ. forward та backward secrecy відповідно). Така ефективність особливо актуальна для груп великих розмірів. І, по-друге, для багатьох сценаріїв необхідно реалізувати таку архітектуру системи комунікацій, яка буде стійкою до відмов у мережі, зокрема не буде містити єдину точку відмови у вигляді центрального сервера. Такі задачі вирішуються за допомогою децентралізованих алгоритмів захищених групових комунікацій.

Багато обчислювальних алгоритмів використовують структуру даних типу дерево, наприклад, для забезпечення можливості розпаралелювання обчислень, керування ієрархією відомостей, сортування, полегшення пошуку інформації, прийняття багатоетапних рішень, синтаксичного аналізу тощо. Враховуючи переваги використання такої структури та необхідність у підвищенні інтелектуальності і захищеності мобільних пристроїв, пропонується дослідити децентралізовані алгоритми захищених групових комунікацій на прикладі групового протоколу Діффі-Хеллмана на основі дерева [2] і проаналізувати їхню ефективність. Детальне порівняння цього алгоритму з аналогами та його переваги наведені у [3].

Щоб дати уявлення про груповий протокол Діффі-Хеллмана на основі дерева, опишемо принцип побудови структури, яка зберігає інформацію про учасників групи та використовується для обчислення спільного групового ключа. Для кожного учасника групи маємо ідентичне збалансоване бінарне дерево, у листових вузлах якого знаходиться інформація про учасників групи та їх публічні ключі. Кожен учасник на початку роботи протоколу має тільки свій власний приватний ключ, який він вибирає

практично довільним чином (враховуються лише обмеження, необхідні для забезпечення бажаного рівня криптографічної стійкості). У проміжних вузлах дерева на вищих рівнях розташовані відповідні приватні та публічні ключі, спільні для їхніх нащадків і необхідні для обчислення спільного групового ключа. Відповідно, у кореневому вузлі бінарного дерева розташований спільний секретний груповий ключ, обчислення якого є основною метою цього протоколу. Деталі роботи протоколу Діффі-Хеллмана на основі дерева можна знайти у [2].

У цій роботі обмежимося розглядом і порівнянням таких основних операцій (без зайвої деталізації) протоколу Діффі-Хеллмана на основі дерева:

• обчислення спільного групового ключа одним учасникам – означає, що цей учасник має актуальне дерево, у якому наявні всі необхідні публічні ключі, і він на основі власного приватного ключа обчислює спільний секретний груповий ключ;

• одиничне приєднання – означає, що до групи приєднується новий учасник, у дереві додається новий листовий вузол (при необхідності й вузли вищих рівнів) та всіма учасниками групи здійснюється переобчислення нового спільного групового ключа;

• одиничний вихід – означає, що з групи вибуває один учасник, відповідний листовий вузол помічається як неактивний (при необхідності і вузли вищих рівнів) та всіма учасниками групи здійснюється переобчислення нового спільного групового ключа;

• масове приєднання – означає, що до групи умовно одночасно входить велика кількість учасників (можна вважати, що більше двох), але особливістю є те, що цю операцію можна ефективно оптимізувати (позбутися зайвих переобчислень після приєднання кожного нового учасника та використати «пакетний» алгоритм (англ. bursty algorithm) [4]);

• масовий вихід – означає, що з групи умовно одночасно виходить велика кількість учасників, і можна застосувати оптимізації, аналогічні тим, що використовуються у операції масового приєднання.

Результати експериментального дослідження

Зазначені вище операції обчислення спільного групового ключа, одиничного приєднання, одиничного виходу, масового приєднання та масового виходу були програмно реалізовані та протестовані за допомогою мобільного пристрою з такими технічними характеристиками: процесор 720 МГц, оперативна пам'ять 256 Мб, операційна система Android.

Обсяг використовуваної оперативної пам'яті на мобільному пристрої при зберіганні структури бінарного дерева зазначеного протоколу становить від 0,556 Мб для групи з 10 учасників до 0,972 Мб для групи з 1000 учасників, що є достатньо економним, враховуючи розмір групи та невелику потужність мобільного пристрою.

Показником швидкодії для наведених далі результатів є реальний час (у мікросекундах, мкс) виконання програмно реалізованих алгоритмів на мобільному пристрої з наведеними вище технічними характеристиками. Результати вимірювання швидкодії обчислення групового ключа одним учасником свідчать про те, що час обчислення змінюється від 1709 мкс для групи з 10 учасників і до 4395 мкс для групи з 1000 учасників, що є досить оптимістичним результатом для такого малопотужного пристрою. Детальні порівняння швидкодії (у розумінні часу виконання) одиничних та оптимізованих масових версій операцій приєднання та виходу учасників для різних розмірів групи наведені у таблиці 1.

Таблиця 1. Час виконання групових операцій залежно від кількості учасників групи на мобільному пристрої з наведеними вище технічними характеристиками

Тип операції \ Розмір групи	**10 учасників**	**100 учасників**	**1000 учасників**
Час створення групи одиничним приєднанням	0 с 17517 мкс	0 с 321625 мкс	6 с 866699 мкс
Час створення групи масовим приєднанням	0 с 12391 мкс	0 с 129181 мкс	1 с 325195 мкс
Час приєднання 1 учасника до існуючої групи	0 с 2167 мкс	0 с 3144 мкс	0 с 11994 мкс
Час видалення 1 учасника з існуючої групи	0 с 122 мкс	0 с 488 мкс	0 с 6226 мкс
Час приєднання 10 учасників до існуючої групи	0 с 13977 мкс	0 с 15046 мкс	0 с 17883 мкс
Час видалення всієї групи (масовий вихід)	0 с 885 мкс	0 с 5158 мкс	0 с 17090 мкс
Час обчислення групового ключа 1 учасником	0 с 1709 мкс	0 с 3051 мкс	0 с 4395 мкс

Висновки

Використання ефективних структур даних, таких як бінарне дерево, та ефективних алгоритмів, таких як груповий протокол Діффі-Хеллмана на основі дерева, дозволяють не тільки реалізовувати нові складні функції мобільних пристроїв, а й якісно підвищувати інтелектуальність таких пристроїв. Зокрема, одним з подальших напрямків розвитку інтелектуальності таких алгоритмів може бути додавання динамічного цифрового підпису, що дозволить контролювати цілісність обчислень та частково наблизитись до вирішення задач, які поставлені перед гомоморфною криптографією та контролем віддалених (делегованих) обчислень.

Як показують результати проведеного експериментального дослідження, децентралізовані групові алгоритми узгодження ключа на основі дерева дозволяють ефективно (у розумінні часу виконання та обсягу використовуваних ресурсів) здійснювати підтримку захищених групових комунікацій на малопотужних мобільних пристроях і, відповідно, дещо розширювати сценарії використання таких пристроїв за рахунок підвищення їхньої інтелектуальності та функціональності.

Література

1. Conti M., Dragoni N., Lesyk V. A Survey of Man In The Middle Attacks / M. Conti, N. Dragoni, V. Lesyk // IEEE Communications Surveys and Tutorials, 18(3). – 2016. – С. 2027-2051.
2. Kim Y. Tree-based group key agreement / Y. Kim, A. Perrig, G. Tsudik // ACM Transactions on Information and System Security, 7(1). – 2004. – С. 60-96.
3. Amir Y. On the performance of group key agreement protocols / Y. Amir, Y. Kim, C. Nita-Rotaru, G. Tsudik // ACM Transactions on Information and System Security, 7(3). – 2004. – С. 457-488.
4. Zou X. Secure group communications over data networks / X. Zou, B. Ramamurthy, S. Magliveras // Springer Science and Business Media. – 2007. – 172 с.

RESUME

A.K. Novokshonov

Increasing intelligence of mobile devices on the example of secure group communication algorithms

The progress of modern mobile technologies not only allows implementing more complex and intelligent algorithms but creates new huge security risks. It happens due to a more important role which modern mobile devices play now (e.g. mobile banking, personal data storage, computational resources, social communications). It is very important to study and analyze algorithms which increase intelligence and security of mobile platforms. In particular, these algorithms may include decentralized secure group communication algorithms. Secure group communications refer to scenarios where trusted members of a group perform information exchange inside the group and need to cryptographically secure (by encryption) this information from external observers. Especially, secure group communications are crucial for distributed applications that work in dynamic environments and perform information exchange over insecure public networks (such as the Internet). Such applications may include multimedia content multicasting, teleconferencing, distance teaching and learning, collaborative work, remote voting, interactive games and information services.

As an example of such decentralized secure group communication protocols, we propose analyzing computational performance of algorithms of the group Diffie-Hellman protocol using an efficient binary tree structure on a low-power mobile device with Android operating system. More specifically, we analyze such operations as group key calculation, single join, single leave, bulk join and bulk leave of group members. The results of computational experiments show that it is feasible to efficiently implement complex algorithms even on low-power mobile devices both in terms of computational complexity and amount of used resources (such as used random access memory). Because of increased intelligence and enhanced security, scenarios of using low-power mobile devices can be somewhat extended.

Надійшла до редакції 10.10.2016

